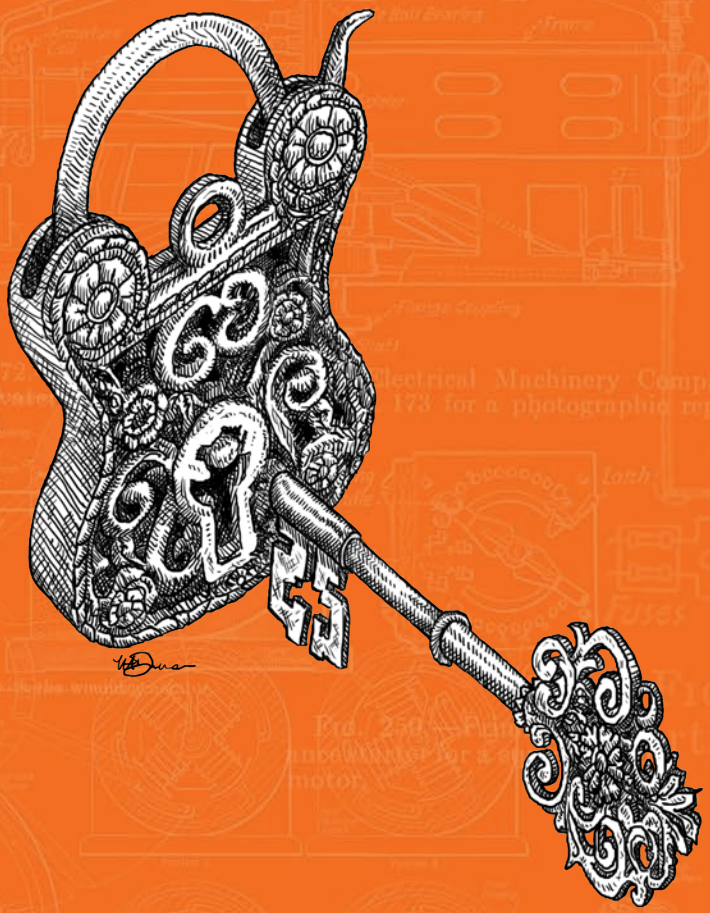
# RFID
# SECURITY TESTING



corsaire
SECURING TRUST

# THE SERVICE

**"Many of the buildings with flawed RFID technology had already been tested by a third-party and given a clean bill of health"**

## WHY WOULD YOU WANT IT?

These days, RFID tokens are used by organisations to regulate access to a diverse range of resources; such as building entry, print management, personnel tracking, and contactless payments.

However, RFID is still relatively new and evolving, which means that the threats are not as well understood in comparison to more-established technologies. Additionally, systems are often supplied as a package or come as part of a leased building, or an outsourcing agreement, and so seem to avoid detailed scrutiny.

RFID Security Testing enables vulnerable systems to be detected and addressed proactively, and in doing so, seeks to avoid costly security breaches and the inevitable, negative publicity.

## WHAT DO WE DO?

Corsaire follows a detailed testing methodology, designed to identify any weaknesses both in the technologies chosen and the implementation. This consists of:

- Enumerating all RFID technologies in use
- Cloning/impersonation evaluation
- Client-side authorisation / privilege escalation
- Vulnerability assessment of known RFID weaknesses
- Brute-forcing of secondary-authentication factors such as PINs
- RFID control software configuration review
- Denial of Service evaluation

When the testing is complete, a detailed report will be generated that includes practical recommendations for improving the security.

For vulnerable systems, a practical demonstration can also be provided to show tokens being covertly captured, then cloned, modified and impersonated.

# CASE STUDY

Corsaire was recently engaged by a client to perform a review of all its key suppliers. In practice, this required all of the critical systems to first be identified, and then audited, including the physical offices.

The majority of the sites reviewed during this project were data centres. These are often treated as physically-secure environments, and have a range of extra security controls installed, on top of those that are normally found in an office.

During one of these reviews, it was identified that the environment relied heavily on RFID technology to identify visitors and also assign role-based access privileges. For example, restricting access to parts of the building, and also making purchases through on-site vending machines. The RFID solution had already been tested several times before by third-parties and had been declared secure.

Once the analysis was started though, a very different story began to unfold. Not only was it possible to clone employee cards and gain access to the site, but due to the particular solution chosen, the communication protocol was also found to be easily intercepted. This meant that the access permissions could be altered, which allowed the cloned card to gain access to areas of the facility that the original could not.

Luckily though, the worst security-issues identified were down to a poorly configured management system. So armed with this knowledge, the owner of the data centre was able to make changes to the software and retain the security investment they had already made.

The real surprise from this project was the misplaced confidence of the data centre operator. Not only had they been misinformed by the original equipment supplier, but also by the third-parties that had tested the environment subsequently. RFID is still a relatively new technology, and the security afforded is often misunderstood. Like all technologies, there are solutions which are inherently stronger than others, and configuration options which can increase the security without having to replace the entire system.

“Our RFID testing solution covers the common technologies and uses, such as access control and asset tracking. This allows an organisation to identify and correct any issues proactively. As a result, not only do they get the most from the existing investment in security systems, but they also avoid any additional costs from a breach, such as an associated fine or negative publicity.”

+44 (0)1483 746 700
GET.IN.TOUCH@CORSAIRE.COM

CORSAIRE LIMITED, UNIT 2 GROSVENOR COURT,
HIPLEY STREET, OLD WOKING, SURREY, GU22 9LL